April 1, 2005

CLMPTO

AS

1. A data transmitting system comprising a data recording medium and a drive unit which accesses the data recording medium,

the data recording medium including:

a security module which executes a mutual authentication protocol with the drive unit and

a recording medium proper; and

the drive unit including:

a controller which executes the mutual authentication protocol when accessing the data recording medium; and

an interface unit which accesses the recording medium proper of the data recording medium.

2. The system as set forth in Claim 1, wherein the mutual authentication protocol uses the public-key encryption technology.

3. The system as set forth in Claim 1, wherein the data recording medium includes the security module and a disc as the data recording medium proper.

4. The system as set forth in Claim 3, wherein the drive unit further includes means for driving the disc as the recording medium proper of the data recording medium.

5. The system as set forth in Claim 1, wherein the interface unit accesses

directly the recording medium proper.

6. The system as set forth in Claim 1, wherein the data recording medium includes the security module and a memory chip as the recording medium proper.

7. The system as set forth in Claim 1, wherein the interface unit accesses the data recording medium via the security module of the data recording medium.

8. The system as set forth in Claim 1, wherein:

the data recording medium has self-identification data stored therein;

the drive unit further includes a storage unit having self-identification data stored therein; and

the security module of the data recording medium and controller of the drive unit exchange their own identification data between them to check whether their counterpart's own identification data is registered in an illegal unit revocation list, when executing the mutual authentication protocol, and will not go through subsequent processes after execution of the mutual authentication protocol if the checking result shows that the drive unit is a unit having to be revoked.

9. The system as set forth in Claim 8, wherein the identification data of the data recording medium is stored in the security module.

10. The system as set forth in Claim 8, wherein the data recording medium has the list stored in the security module thereof.

11. The system as set forth in Claim 8, wherein the data recording medium has the list stored in the recording medium proper thereof.

12. The system as set forth in Claim 8, wherein the drive unit has the list stored in the storage unit thereof.

13. The system as set forth in Claim 8, wherein the drive unit has not the list stored in the storage unit thereof.

14. The system as set forth in Claim 8, wherein there is executed a mutual authentication protocol corresponding to whether either or both of the security module and drive unit itself holds the list or not.

15. The system as set forth in Claim 8, wherein the controller of the drive unit judges whether or not the data recording medium is a one whose security module has the list stored therein, and executes a mutual authentication protocol which is based on the judgment result.

16. The system as set forth in Claim 8, wherein the security module of the data recording medium judges whether or not the drive unit is a one having the list stored therein, and executes a mutual authentication protocol which is based on the judgment result.

17. The system as set forth in Claim 8, wherein:

the data recording medium has stored therein the list version number and the list itself;

the drive unit has the list version number and the list itself stored in the storage unit thereof; and

drive unit exchange the version numbers of their own lists between them when executing the mutual authentication protocol, and one of them whichever has a newer list sends the list to the other while the other having an older list updates its list with the received new list.

18. The system as set forth in Claim 8, wherein:

the data recording medium has the list version number stored therein and the list itself recorded in the recording medium proper thereof;

the drive unit has the list version number and the list itself stored in the storage unit thereof;

the security module of the data recording medium and controller of the drive unit exchange the version numbers of their own revocation lists between them when executing the mutual authentication protocol; and

the drive unit will write the list to the data recording medium when the list stored in the storage unit of the drive unit is newer, while it will read the list from the data recording medium and update its own list with the list read from the data recording medium when its own list is older.

19. The system as set forth in Claim 8, wherein both the drive unit and security module check, using their own new lists, whether or not their counterpart's identification data are registered in the lists, respectively.

20. The system as set forth in Claim 1, wherein:

the drive unit further includes a storage unit having self-identification data

21. The system as set forth in Claim 1, wherein:

the data recording medium has self-identification data stored therein; and

the controller of the drive unit receives the identification data from the security module and checks whether or not the identification data of the security module is registered in the illegal unit revocation list, when executing the mutual authentication protocol, and will not go through subsequent processes after execution of the mutual authentication protocol if the checking result shows that the drive unit is a unit having to be revoked.

22. (Amended) The system as set forth in Claim 8, wherein the illegal unit revocation list has registered therein identification data of units having to be revoked and a unit registered in this list is taken as having to be revoked.

23. (Amended) The system as set forth in Claim 8, wherein the illegal unit revocation list has registered therein identification data of units having not to be revoked and a unit not registered in the list is taken as having to be revoked.

24. (Amended) The system as set forth in Claim 8, wherein the illegal unit revocation list includes:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

a unit registered in the revocation list and/or not registered in the registration list being taken as having to be revoked.

25. (Amended) The system as set forth in Claim 8, wherein the illegal unit revocation list consists of:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

either of the revocation and registration lists being selected to judge whether or not a unit in consideration is a on having to be revoked.

26. The system as set forth in Claim 1, wherein when executing the mutual authentication protocol, the drive unit and security module execute a key sharing protocol using the public-key encryption technology, encrypt a data encrypting content key with a shared key thus obtained, and send the encrypted content key

from one of them to the other.

27. The system as set forth in Claim 1, wherein when executing the mutual authentication protocol, the drive unit and security module execute a key sharing protocol using the public-key encryption technology, encrypt data with a shared key thus obtained, and send the encrypted data from one of them to the other.

28. The system as set forth in Claim 1, wherein:

the drive unit is to write data to the recording medium proper via the interface unit;

the drive unit and security module execute a key sharing protocol using the public-key encryption technology;

the drive unit encrypts a data encrypting content key with a shared key obtained of the key sharing protocol and sends the encrypted data encrypting content key to the security module; and

the security module decrypts the encrypted content key received from the drive unit with the shared key obtained of the key sharing protocol, re-encrypts the decrypted content key with a save key stored therein and sends the re-encrypted content key to the drive unit; and

the drive unit writes to the recording medium proper via the interface unit the data encrypted with the content key and the content key encrypted by the security module using the save key.

29. The system as set forth in Claim 1, wherein:

the drive unit is to read data from the recording medium proper via the interface unit;

the drive unit and security module execute a key sharing protocol using the public-key encryption technology;

the drive unit reads the encrypted content key from the recording medium proper and sends the read content key to the security module;

the security module decrypts the encrypted content key received from the drive unit with the save key stored therein, re-encrypts the decrypted content key with the shared key obtained of the key sharing protocol and sends the re-encrypted content key to the drive unit; and

the drive unit decrypts the encrypted content key received from the security module with the shared key obtained of the key sharing protocol, reads the content key-encrypted data from the recording medium proper and decrypts the read data.

30. The system as set forth in Claim 1, wherein:

the drive unit is to write data to the recording medium proper via the interface unit;

the interface unit accesses the recording medium proper via the security module of the data recording medium;

the drive unit and security module execute a key sharing protocol using the public-key encryption technology;

the drive unit sends to the security module a data encrypting content key and having been encrypted with a shared key obtained of the key sharing protocol and data encrypted with the content key; and

the security module decrypts the encrypted content key received from the drive unit with the shared key obtained through the execution of the key sharing protocol and records to the recording medium proper the content key re-encrypted with a save key stored in the security module and data encrypted with the content key received from the drive unit.

31. The system as set forth in Claim 1, wherein:

the drive unit is to write data to the recording medium proper via the interface unit;

the interface unit accesses the recording medium proper via the security module of the data recording medium;

the drive unit and security module execute a key sharing protocol using the public-key encryption technology;

the drive unit encrypts data with a shared key obtained through the execution of the key sharing protocol and sends the data thus encrypted to the security module; and

the security module decrypts the encrypted data received from the drive unit with the shared key, encrypts the decrypted data and stores the encrypted data into the recording medium proper.

32. The system as set forth in Claim 1, wherein:

the drive unit is to read data from the recording medium proper via the interface unit;

the interface unit accesses the recording medium proper via the security module of the data recording medium;

the drive unit and security module execute a key sharing protocol using the public-key encryption technology;

the security module reads from the recording medium proper an encrypted content key and data encrypted with the content key, decrypts the encrypted content key with a save key stored therein and sends to the drive unit the content key re-encrypted with a shared key obtained through the execution of the key sharing protocol and data encrypted with the content key read from the recording medium proper; and

the drive unit decrypts the encrypted content key received from the security module with the shared key obtained through the execution of the key sharing protocol and decrypts the encrypted data with the content key.

33. The system as set forth in Claim 1, wherein:

the drive unit is to read data from the recording medium proper via the interface unit;

the interface unit accesses the recording medium proper via the security module of the data recording medium;

the drive unit and security module execute a key sharing protocol using the public-key encryption technology;

the security module reads data encrypted and stored in the data recording medium, decrypts the encrypted data with the content key, re-encrypts the decrypted data by the user of the shared key obtained through the execution of the key sharing protocol and sends the re-encrypted data to the drive unit; and

the drive unit decrypts, with the shared key obtained through the execution of the key sharing protocol, the encrypted data received from the security module.

34. A data transmitting method for transferring data between a data recording medium having a recording medium proper and a drive unit which accesses the data recording medium, the method comprising steps of:

executing a mutual authentication protocol between a controller provided in the drive unit and a security module provided in the data recording medium; and

accessing, by the drive unit, the recording medium proper of the data recording medium according to the result of the mutual authentication protocol execution.

35. The method as set forth in Claim 34, wherein the mutual authentication protocol is a protocol using the public-key encryption technology.

36. The method as set forth in Claim 34, wherein the interface unit of the drive unit accesses directly the recording medium proper.

37. The method as set forth in Claim 34, wherein the interface unit of the drive

unit accesses the data recording medium via the security module of the data recording medium.

38. The method as set forth in Claim 34, wherein:

the data recording medium has self-identification data stored therein;

the drive unit further includes a storage unit having self-identification data stored therein; and

the security module of the data recording medium and controller of the drive unit exchange their own identification data between them to check whether their counterpart's identification data is registered in an illegal unit revocation list, when executing the mutual authentication protocol, and will not go through subsequent processes after execution of the mutual authentication protocol if the checking result shows that the drive unit is a unit having to be revoked.

39. The method as set forth in Claim 38, wherein the data recording medium has the identification data stored in the security module thereof.

40. The method as set forth in Claim 38, wherein the data recording medium has the list stored in the security module thereof.

41. The method as set forth in Claim 38, wherein the data recording medium has the list stored in the recording medium proper thereof.

42. The method as set forth in Claim 38, wherein the drive unit has the list stored in the storage unit thereof.

43. The method as set forth in Claim 38, wherein the drive unit has not the list

stored in the storage unit thereof.

44. The method as set forth in Claim 38, wherein there is executed a mutual authentication protocol corresponding to whether either or both of the drive unit and data recording medium holds the above list or not.

45. The method as set forth in Claim 38, wherein the controller of the drive unit judges whether or not the data recording medium is a one whose security module has the list stored therein, and executes a mutual authentication protocol which is based on the judgment result.

46. The system as set forth in Claim 38, wherein the security module of the data recording medium judges whether or not the drive unit is a one having the list stored therein, and executes a mutual authentication protocol which is based on the judgment result.

47. The method as set forth in Claim 38, wherein:

the data recording medium has stored therein the list version number and the list itself;

the storage unit of the drive unit stores the list version number and list itself therein; and

the security module of the data recording medium and controller of the drive unit exchange the version numbers of their own revocation lists between them when executing the mutual authentication protocol, and one of them whichever has a new list sends the list to the other while the other having the old

list updates its list with the received new list.

48. The method as set forth in Claim 38, wherein:

the data recording medium has the list version number stored therein and the list itself recorded in the recording medium proper thereof;

the drive unit has the list version number and list itself stored in the storage unit thereof;

the security module of the data recording medium and controller of the drive unit exchange the version numbers of their own revocation lists between them when executing the mutual authentication protocol; and

the drive unit writes the list to the data recording medium when the list stored in the storage unit thereof is a new one while the drive unit reads the list from the data recording medium and update its own list with the list read from the data recording medium when the list in the drive unit is an old one.

49. The method as set forth in Claim 38, wherein both the drive unit and security module check, using their own new lists, whether or not their counterpart's identification data are registered in the lists, respectively.

50. The method as set forth in Claim 34, wherein:

the drive unit further includes a storage unit having self-identification data stored therein; and

the security module of the data recording medium receives the identification data from the drive unit and checks whether or not the identification data of the drive unit is registered in the illegal unit revocation list, when executing the mutual authentication protocol, and will not go through subsequent processes after execution of the mutual authentication protocol if the checking result shows that the drive unit is a unit having to be revoked.

51. The method as set forth in Claim 34, wherein:

the data recording medium has self-identification data stored therein; and

the controller of the drive unit receives the identification data from the security module and checks whether or not the identification data of the security module is registered in the illegal unit revocation list, when executing the mutual authentication protocol, and will not go through subsequent processes after execution of the mutual authentication protocol if the checking result shows that the drive unit is a unit having to be revoked.

52. (Amended) The method as set forth in Claim 38, wherein the illegal unit revocation list has registered therein identification data of units having to be revoked and a unit registered in this list is taken as having to be revoked.

53. (Amended) The method as set forth in Claim 38, wherein the illegal unit revocation list has registered therein identification data of units having not to be revoked and a unit not registered in the list is taken as having to be revoked.

54. (Amended) The method as set forth in Claim 38, wherein the illegal unit revocation list consists of:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

a unit registered in the revocation list and/or not registered in the registration list being taken as having to be revoked.

55. (Amended) The method as set forth in Claim38, wherein the illegal unit revocation list consists of:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

either of the revocation and registration lists being selected to judge whether or not a unit in consideration is included in the units having to be revoked.

56. The method as set forth in Claim 34, wherein when executing the mutual authentication protocol, the drive unit and security module execute a key sharing protocol using the public-key encryption technology, encrypt a data encrypting content key with a shared key thus obtained, and send the encrypted content key from one of them to the other.

57. The method as set forth in Claim 34, wherein when executing the mutual authentication protocol, the drive unit and security module execute a key sharing

protocol using the public-key encryption technology, encrypt data with a shared key thus obtained, and send the encrypted data from one of them to the other.

58. The method as set forth in Claim 34, wherein:

the drive unit is to write data to the recording medium proper;

the drive unit and security module execute the key sharing protocol using the public-key encryption technology;

the drive unit encrypts the data content key with the shared key obtained through the execution of the key sharing protocol and sends the encrypted content key to the security module; and

the security module decrypts the encrypted content key received from the drive unit with the shared key obtained through the execution of the key sharing protocol, re-encrypts the content key decrypted with a save key stored therein and transmits the re-encrypted content key to the drive unit; and

the drive unit writes to the recording medium proper the data encrypted with the content key and the content key encrypted by the security module using the save key.

59. The method as set forth in Claim 34, wherein:

the drive unit is to read data from the recording medium proper;

the drive unit and security module execute the key sharing protocol using the public-key encryption technology;

the drive unit reads the encrypted content key from the recording medium

proper and sends the read content key to the security module; and

the security module decrypts the encrypted content key received from the drive unit with the save key stored therein, re-encrypts the decrypted content key with the shared key obtained through the execution of the key sharing protocol and sends it to the drive unit; and

the drive unit decrypts the encrypted content key received from the security module with the shared key obtained through the execution of the key sharing protocol, reads the data encrypted with the content key from the recording medium proper and decrypts the read data.

60. The method as set forth in Claim 34, wherein:

the drive unit is to write data to the recording medium proper via the interface unit;

the interface unit accesses the recording medium proper via the security module of the data recording medium;

the drive unit and security module execute the key sharing protocol using the public-key encryption technology;

the drive unit sends to the security module the data content key encrypted with the shared key obtained through the execution of the key sharing protocol and data encrypted with the content key; and

the security module decrypts the encrypted content key received from the drive unit with the shared key obtained through the execution of the key sharing

protocol and writes to the recording medium proper the content key re-encrypted with the save key stored in the security module and data encrypted with the content key received from the drive unit.

61. The method as set forth in Claim 34, wherein:

the drive unit is to write data to the recording medium proper via the interface unit;

the interface unit accesses the recording medium proper via the security module of the data recording medium;

the drive unit and security module execute the key sharing protocol using the public-key encryption technology;

the drive unit encrypts data with the shared key obtained through the execution of the key sharing protocol and sends the data thus encrypted to the security module; and

the security module decrypts, with the shared key, the encrypted data received from the drive unit, encrypts the decrypted data and stores the encrypted data to the recording medium proper.

62. The method as set forth in Claim 34, wherein:

the drive unit is to read the encrypted data from the recording medium proper via the interface unit;

the interface unit accesses the recording medium proper via the security module of the data recording medium;

the drive unit and security module execute the key sharing protocol using the public-key encryption technology;

the security module reads from the recording medium proper the encrypted content key and data encrypted with the content key, decrypts the encrypted content key with the save key stored therein and sends to the drive unit the content key re-encrypted with the shared key obtained through the execution of the key sharing protocol and data encrypted with the content key read from the recording medium proper; and

the drive unit decrypts, with the shared key obtained through the execution of the key sharing protocol, the encrypted content key received from the security module and decrypts the encrypted data with the content key.

63. The method as set forth in Claim 34, wherein:

the drive unit is to read data from the recording medium proper via the interface unit;

the interface unit accesses the recording medium proper via the security module of the data recording medium;

the drive unit and security module execute the key sharing protocol using the public-key encryption technology;

the security module reads data encrypted and stored in the data recording medium, decrypts the encrypted data with the content key, re-encrypts the decrypted data with the shared key obtained through the execution of the key

sharing protocol and sends the re-encrypted data to the drive unit; and

the drive unit decrypts the encrypted data received from the security module with the shared key obtained through the execution of the key sharing protocol.

64. A drive unit which accesses a data recording medium including a recording medium proper and a security module which executes a mutual authentication protocol with the drive unit, the drive unit comprising:

a controller which executes the mutual authentication protocol when accessing the data recording medium; and

an interface unit which accesses the recording medium proper of the data recording medium.

65. The drive unit as set forth in Claim 64, wherein the mutual authentication protocol is a protocol using the public-key encryption technology.

66. The drive unit as set forth in Claim 64, further comprising a drive means for driving a disc as the recording medium proper of the data recording medium.

67. The drive unit as set forth in Claim 64, wherein the interface unit accesses a memory chip as the recording medium proper of the recording medium.

68. The drive unit as set forth in Claim 64, wherein the interface unit accesses directly the recording medium proper.

69. The drive unit as set forth in Claim 64, wherein the interface unit accesses the recording medium proper of the data recording medium via the security module of the data recording medium.

70. The drive unit as set forth in Claim 64, further comprising a storage unit having self-identification data stored therein, wherein when executing the mutual authentication protocol, the controller sends the identification data stored in the storage unit to the security module while receiving, from the security module, the self-identification data stored in the data recording medium, to thereby check whether their counterpart's identification data are registered in respective illegal unit revocation lists, and will not go through subsequent processes after execution of the mutual authentication protocol if the checking result shows that the drive unit is a one having to be revoked.

71. The drive unit as set forth in Claim 70, having the list stored in the storage unit thereof.

72. The drive unit as set forth in Claim 70, having the list not stored in the storage unit thereof.

73. The drive unit as set forth in Claim 70, wherein there is executed a mutual authentication protocol corresponding to whether either or both of the security module and drive unit itself holds the above respective lists or not.

74. The drive unit as set forth in Claim 70, wherein the controller of the drive unit judges whether or not the data recording medium is a one whose security module has the list stored therein, and executes a mutual authentication protocol which is based on the judgment result.

75. The drive unit as set forth in Claim 70, wherein:

the storage uni thereof has stored therein the list version number and the list itself; and

the controller transmits, when executing the mutual authentication protocol, the list version number stored in the storage unit to the security module while receiving, from the security module, the list version number the data recording medium holds therein, and sends, when its list is a new one, the list to the security module while updating, when its list is an old one, the list with the new list received from the security module.

76. The drive unit as set forth in Claim 70, wherein:

the storage uni has stored therein the list version number and the list itself; and

the controller transmits, when executing the mutual authentication protocol, the list version number stored in the storage unit to the security module while receiving, from the security module, the list version number the data recording medium holds therein, and writes, when its list is a new one, the list to the recording medium proper of the data recording medium while reading, when its list is an old one, the list recorded in the recording medium proper of the data recording medium, and updating its list with the read list.

77. The drive unit as set forth in Claim 70, adapted to work with the security module in checking, using their own new lists, whether or not their counterpart's identification data are registered in their own lists, respectively.

78. The drive unit as set forth in Claim 64, wherein when executing the mutual authentication protocol, the controller receives, from the security module, the self-identification data held in the data recording medium, checks whether or not the identification data of the security module is registered in the illegal unit revocation list, and will not go through subsequent processes after execution of the mutual authentication protocol if the checking result shows that the drive unit is a unit having to be revoked.

79. (Amended) The drive unit as set forth in Claim 70, wherein the illegal unit revocation list has registered therein identification data of units having to be revoked and the units registered in this list are taken as having to be revoked.

80. (Amended) The drive unit as set forth in Claim 70, wherein the illegal unit revocation list has registered therein identification data of units having not to be revoked and a unit not registered in the list is taken as having to be revoked.

81. (Amended) The drive unit as set forth in Claim 70, wherein the illegal unit revocation list consists of:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

a unit registered in the revocation list and/or not registered in the registration list being taken as having to be revoked.

82. (Amended) The drive unit as set forth in Claim 70, wherein the illegal unit revocation list consists of:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

either of the revocation and registration lists being selected to judge whether or not a unit in consideration is included in the listed units having to be revoked.

83. The drive unit as set forth in Claim 64, adapted to work with the security module, when executing the mutual authentication protocol, in executing a key sharing protocol using the public-key encryption technology, encrypt a data encrypting content key with a shared key thus obtained, and send the encrypted content key from one of the drive unit and security module to the other.

84. The drive unit as set forth in Claim 64, adapted to work with the security module, when executing the mutual authentication protocol, in executing a key sharing protocol using the public-key encryption technology, encrypt data with a shared key thus obtained, and send the encrypted data from one of the drive unit and security module to the other.

85. The drive unit as set forth in Claim 64, destined to write data to the recording medium proper via the interface unit, wherein:

a protocol for key sharing with the security module is executed using the

public-key encryption technology;

the data content key is encrypted with the shared key obtained through the execution of the key sharing protocol and the encrypted data content key is sent to the security module;

the security module decrypts the encrypted content key with the shared key obtained through the execution of the key sharing protocol, and receives data re-encrypted with the content key decrypted with save key stored therein; and

the data encrypted with the content key and the content key encrypted by the security module using the save key are recorded to the recording medium proper via the interface unit.

86. The drive unit as set forth in Claim 64, destined to read encrypted data from the recording medium proper via the interface unit, wherein:

a protocol for key sharing with the security module is executed using the public-key encryption technology;

the encrypted content key is read from the recording medium proper and the read content key is sent to the security module; and

the security module decrypts the encrypted content key with the shared key obtained through the execution of the key sharing protocol and receives data re-encrypted with the content key decrypted with the shared key obtained through the execution of the key sharing protocol; and

the encrypted content key received from the security module is decrypted

with the shared key obtained through the execution of the key sharing protocol, the data encrypted with the content key is read from the recording medium proper and decrypted.

87. The drive unit as set forth in Claim 64, destined to record data.to the recording medium proper via the interface unit, wherein:

the interface unit accesses the recording medium proper via the security module of the data recording medium;

a protocol for key sharing with the security module is executed using the public-key encryption technology;

the data content key encrypted with the shared key obtained through the execution of the key sharing protocol and data encrypted with the content key are sent to the security module; and

the security module decrypts the encrypted content key with the shared key obtained through the execution of the key sharing protocol and writes to the recording medium proper the content key re-encrypted with the save key stored in the security module and data encrypted with the content key.

88. The drive unit as set forth in Claim 64, destined to write data to the recording medium proper via the interface unit, wherein

the interface unit accesses the recording medium proper via the security module of the data recording medium;

a protocol for key sharing with the security module is executed using the

public-key encryption technology;

data is encrypted with the shared key obtained through the execution of the key sharing protocol and sent to the security module; and

the security module decrypts the encrypted data with the shared key, encrypts the decrypted data with the content key and stores the encrypted data to the recording medium proper.

89. The drive unit as set forth in Claim 64, destined to read data from the recording medium proper via the interface unit, wherein:

the interface unit accesses the recording medium proper via the security module of the data recording medium;

a protocol for key sharing with the security module is executed using the public-key encryption technology;

the security module reads from the recording medium proper the encrypted content key and data encrypted with the content key, decrypts the encrypted content key with the save key stored therein and receives the content key re-encrypted with the shared key obtained through the execution of the key sharing protocol and data encrypted with the content key read from the recording medium proper; and

the encrypted content key received from the security module is decrypted with the shared key obtained through the execution of the key sharing protocol and the encrypted data is decrypted with the content key.

90. The drive unit as set forth in Claim 64, destined to read data from the recording medium proper via the interface unit, wherein:

the interface unit accesses the recording medium proper via the security module of the data recording medium;

a protocol for key sharing with the security module is executed using the public-key encryption technology;

the security module reads data encrypted and stored in the data recording medium, decrypts the encrypted data with the content key, receives data resulted from re-encryption of the decrypted data with the shared key obtained through the execution of the key sharing protocol; and

the encrypted data received from the security module is decrypted with the shared key obtained through the execution of the key sharing protocol.

91. An access method for access to a data recording medium including a recording medium proper and a security module which executes a mutual authentication protocol with a drive unit, the method comprising steps of:

executing the mutual authentication protocol when accessing the data recording medium; and

accessing the recording medium proper of the data recording medium according to the result of the mutual authentication protocol execution.

92. The method as set forth in Claim 91, wherein the mutual authentication protocol is a protocol using the public-key encryption technology.

93. The method as set forth in Claim 91, where access is made to a memory chip as the recording medium proper of the data recording medium.

94. The method as set forth in Claim 91, wherein access is made directly to the recording medium proper.

95. The method as set forth in Claim 91, wherein the interface unit accesses the data recording medium via the security module of the data recording medium.

96. The method as set forth in Claim 91, wherein:

the drive unit stores self-identification data;

the drive unit and the security module of the data recording medium exchange, between them, the self-identification data stored in the drive unit and the identification data stored in the data recording medium, when executing the mutual authentication protocol, to check whether their counterpart's identification data is registered in an illegal unit revocation list, and will not go through subsequent processes after execution of the mutual authentication protocol if the checking result shows that the drive unit is a unit having to be revoked.

97. The method as set forth in Claim 96, wherein there is executed a mutual authentication protocol corresponding to whether either or both of the security module and drive unit itself holds the above list or not.

98. The method as set forth in Claim 96, wherein the controller of the drive unit judges whether or not the data recording medium is a one whose security module has the list stored therein, and executes a mutual authentication protocol which is

based on the judgment result.

99. The method as set forth in Claim 96, wherein:

the data recording medium has stored therein the list version number and the list itself and the drive unit has the list version number and list itself stored in the storage unit thereof; and

the security module of the data recording medium and controller of the drive unit exchange the version numbers of their own revocation lists between them when executing the mutual authentication protocol, and one of them whichever has a new list sends the list to the other while the other having the old list updates its list with the received new list.

100. The method as set forth in Claim 96, wherein:

the data recording medium has the list version number stored therein and the list itself recorded in the recording medium proper thereof and the drive unit has the list version number and list itself stored in the storage unit thereof;

the security module of the data recording medium and controller of the drive unit exchange the version numbers of their own revocation lists between them when executing the mutual authentication protocol; and

the drive unit will write the list to the data recording medium when the list stored in the storage unit of the drive unit is a new one while the drive unit will read the list from the data recording medium and update its own list using the list read from the data recording medium when the list in the drive unit is an old one.

101. The method as set forth in Claim 96, wherein both the drive unit and security module check, using their own new lists, whether or not their counterpart's identification data are registered in the lists, respectively.

102. The method as set forth in Claim 91, wherein:

the security module of the data recording medium receives the identification data from the drive unit and checks whether or not the identification data of the drive unit is registered in the illegal unit revocation list, when executing the mutual authentication protocol, and will not go through subsequent processes after execution of the mutual authentication protocol if the checking result shows that the drive unit is a unit having to be revoked.

103. (Amended) The method as set forth in Claim 96, wherein the illegal unit revocation list has registered therein identification data of units having to be revoked and a unit registered in this list is taken as having to be revoked.

104. (Amended) The method as set forth in Claim 96, wherein the illegal unit revocation list has registered therein identification data of units having not to be revoked and a unit not registered in the list is taken as having to be revoked.

105. (Amended) The method as set forth in Claim 96, wherein the illegal unit revocation list consists of:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

a unit registered in the revocation list and/or not registered in the registration list being taken as having to be revoked.

106. (Amended) The method as set forth in Claim 96, wherein the illegal unit revocation list consists of:

a revocation list having registered therein identification data of units having to be revoked; and

a registration list having registered therein identification data of units having not to be revoked;

either of the revocation and registration lists being selected to judge whether or not the drive unit is included in the units having to be revoked.

107. The method as set forth in Claim 91, wherein when executing the mutual authentication protocol, the drive unit and security module execute a key sharing protocol using the public-key encryption technology, encrypt, using a shared key thus obtained, a data encrypting content key, and send the encrypted content key from one of them to the other.

108. The method as set forth in Claim 91, wherein when executing the mutual authentication protocol, the drive unit and security module execute a key sharing protocol using the public-key encryption technology, encrypt data with a shared key thus obtained, and send the encrypted data from one of them to the other.

109. The method as set forth in Claim 91, wherein:

the drive unit and security module execute the key sharing protocol using the public-key encryption technology;

the drive unit encrypts the data content key with the shared key obtained through the execution of the key sharing protocol and sends the encrypted data content key to the security module; and

the security module decrypts the encrypted content key received from the drive unit with the shared key obtained through the execution of the key sharing protocol, re-encrypts the content key decrypted with a save key stored therein and transmits the re-encrypted content key to the drive unit; and

the drive unit writes to the recording medium proper via the interface unit the data encrypted with the content key and the content key encrypted by the security module using the save key.

110. The method as set forth in Claim 91, wherein:

the drive unit and security module execute the key sharing protocol using the public-key encryption technology;

the drive unit reads the encrypted content key from the recording medium proper and sends the read content key to the security module; and

the security module decrypts the encrypted content key with the save key stored in the security module, and receive data obtained by re-encrypting the decrypted content key with the shared key obtained through the execution of the

key sharing protocol; and

the drive unit decrypts, with the shared key obtained through the execution of the key sharing protocol, the encrypted content key received from the security module, reads the data encrypted with the content key from the recording medium proper and decrypts the read data.

111. The method as set forth in Claim 91, wherein:

the interface unit accesses the recording medium proper via the security module of the data recording medium;

the drive unit and security module execute the key sharing protocol using the public-key encryption technology;

the drive unit sends to the security module the data content key encrypted with the shared key obtained through the execution of the key sharing protocol and data encrypted with the content key; and

the security module decrypts the encrypted content key received from the drive unit with the shared key obtained through the execution of the key sharing protocol and writes to the recording medium proper the content key re-encrypted with the save key stored in the security module and data encrypted with the content key received from the drive unit.

112. The method as set forth in Claim 91, wherein:

the interface unit accesses the recording medium proper via the security module of the data recording medium;

the drive unit and security module execute the key sharing protocol using

the public-key encryption technology;

the drive unit encrypts data with the shared key obtained through the execution of the key sharing protocol and sends the data thus encrypted to the security module; and

the security module decrypts, with the shared key, the encrypted data received from the drive unit, encrypts the decrypted data and stores the encrypted data to the recording medium proper.

113. The method as set forth in Claim 91, wherein:

the interface unit accesses the recording medium proper via the security module of the data recording medium;

the drive unit and security module execute the key sharing protocol using the public-key encryption technology;

the security module reads from the recording medium proper the encrypted content key and data encrypted with the content key, decrypts the encrypted content key with the save key stored therein and sends to the drive unit the content key re-encrypted with the shared key obtained through the execution of the key sharing protocol and data encrypted with the content key read from the recording medium proper; and

the drive unit decrypts, with the shared key obtained through the execution of the key sharing protocol, the encrypted content key received from the security module and decrypts the encrypted data with the content key.

114. The method as set forth in Claim 91, wherein:

the interface unit accesses the recording medium proper via the security module of the data recording medium;

the drive unit and security module execute the key sharing protocol using the public-key encryption technology;

the security module reads data encrypted and stored in the data recording medium, decrypts the encrypted data with the content key, re-encrypts the decrypted data with the shared key obtained through the execution of the key sharing protocol and sends the re-encrypted data to the drive unit; and

the drive unit decrypts, with the shared key obtained through the execution of the key sharing protocol, the encrypted data received from the security module.

115. A data recording medium having a data recording area, comprising:

a security module having an interface function for interfacing with an external unit, a random number generating function, a data storing function, and a calculating function to provide a necessary calculation for mutual authentication protocol using the public-key encryption technology; and

a recording medium proper having the data recording area.

116. The data recording medium as set forth in Claim 115, wherein the security module further includes an interface function to access the data recording medium proper.

117. An access method for access to a data recording medium having a data

recording area, the method comprising steps of:

connecting to an external unit;

generating a random number and sending it to the external unit;

making, using data received from the external unit and stored data, a necessary calculation for a protocol, for mutual authentication with the external unit, using the public-key encryption technology;

executing the mutual authentication mutual authentication protocol with the external unit; and

accessing a recording medium proper, in which data is to be recorded, of the data recording medium according to the result of the mutual authentication protocol execution.

118. A recording medium producing apparatus for producing a data recording medium, comprising:

a recording unit to record an illegal unit revocation list to the data recording medium which includes a recording medium proper in which data is to be recorded and a security module which executes a mutual authentication mutual authentication protocol with a drive unit which accesses the recording medium proper of the data recording medium.

119. The unit as set forth in Claim 118, further comprising an assembling unit to assemble the data recording medium including the security module and recording medium proper.

120. The unit as set forth in Claim 118, wherein the recording unit records the list into the security module.

121. The unit as set forth in Claim 118, wherein the recording unit records the list version number and the list itself into the security module.

122. The unit as set forth in Claim 118, wherein the recording unit records the list in the recording medium proper.

123. The unit as set forth in Claim 118, wherein the recording unit records the list version number into the security module and the list itself in the recording medium proper.

124. The unit as set forth in Claim 118, wherein the recording unit records, into the security module, the identification data of the data recording medium, private key and public key certificates which are to be used in the public-key encryption technology given in the data recording medium, and the list version number.

125. The unit as set forth in Claim 118, wherein the recording unit further comprises means for storing the list which is to be recorded to the data recording medium.

126. The unit as set forth in Claim 118, wherein the recording unit further comprises an interface through which the list to be recorded into the data recording medium is acquired.

127. The unit as set forth in Claim 118, wherein the list is composed of a

revocation list having registered therein identification data of units having to be revoked and/or a registration list having registered therein identification data of units having not to be revoked.

128. A recording medium producing method for producing a data recording medium, comprising a step of:

recording an illegal unit revocation list to the data recording medium which includes a recording medium proper in which data is to be recorded and a security module which executes a mutual authentication mutual authentication protocol with a drive unit which accesses the recording medium proper of the data recording medium.

129. The method as set forth in Clam 128, in which the data recording medium including the security module and recording medium proper is assembled.

130. The method as set forth in Claim 128, wherein the list is recorded into the security module.

131. The method as set forth in Claim 128, wherein the list version number and the list itself are recorded into the security module.

132. The method as set forth in Claim 128, wherein the list is recorded to the recording medium proper.

133. The method as set forth in Claim 128, wherein the list version number is recorded into the security module while the list itself is recorded to the recording medium proper.

134. The method as set forth in Claim 128, wherein the identification data of the data recording medium, private and public key certificates which are to be used in the public-key encryption technology given in the data recording medium, and the list are recorded into the security module.

135. The method as set forth in Claim 128, wherein the list is stored into the data recording medium.

136. The method as set forth in Claim 128, wherein the list to be recorded into the data recording medium is acquired from outside.

137. The method as set forth in Claim 128, wherein the list is composed of a revocation list having registered therein units having to be revoked and/or a registration list having registered therein units having not to be revoked.